Definition 1. A *group* is a non-empty set G together with an operation, called *multiplication*, which associates with each ordered pair x, y of elements in G a third element, their *product*, in G such that,

1. multiplication is *associative*;
2. there exists an *identity element* e in G; and
3. for each element x in G there exists an *inverse* of x.

In other words, for x and y in G there exists xy in G such that,

1. for any x, y and z in G, $x(yz) = (xy)z$;
2. there exists e in G such that $xe = ex = x$; and
3. to each x in G there corresponds x^{-1} in G such that $xx^{-1} = x^{-1}x = e$.

A group is called *Abelian* or *commutative group* if $xy = yx$ for all elements x and y in G. The group G is called a *finite group* if it consists of a finite number of elements, otherwise it is called an *infinite group*. This number of elements of G is called its *order*.

Theorem 1. Both the identity e and the inverse x^{-1} of a group G are unique.

Proof. Suppose e' is another element in G such that $xe' = e'x = x$ for every x in G, then $e' = e'e = e$, hence the identity element is unique. Suppose for every x in G, that x' be another element in G such that $xx' = x'x = e$, then,

$$x' = x'e = x'(xx^{-1}) = (x'x)x^{-1} = ex^{-1} = x^{-1}$$

hence the inverse element of G is unique.

Definition 2. A *ring* is an additive Abelian group R which is closed under a second operation, called *multiplication*, in such a manner that,

1. multiplication is *associative*; and
2. multiplication is *distributive*.

That is to say, if x, y and z are any three elements in R, then,

1. $x(yz) = (xy)z$; and
2. $x(y+z) = xy + xz$ and $(x+y)z = xz + yz$.

A ring is called a *commutative ring* if $xy = yx$ for all elements x and y in R. If a ring R has a non-zero element 1 with such a property that $x1 = 1x = x$ for every x, then 1 is called an *identity element*, and R is said to be a *ring with identity*.

Definition 3. Let x be an element of R, a ring with identity. Then x is said to be *regular* if its inverse x^{-1} exists, otherwise it is said to be *singular*. Regular elements are also called *invertible-* or *non-singular* elements. Furthermore, R is called a *division ring* if all its non-zero elements are regular.

§

Definition 4. A *field* is a commutative division ring.

Example 1. A field, then, is a non-empty set F together with two operations on its elements, namely addition and multiplication, such that for all a, b and c in F, under addition, F is closed, commutative, associative, has a unique identity, has for each of its elements a unique inverse; and under multiplication, F is closed, commutative, associative, has a unique identity, has for each of its elements a unique inverse. Furturemore, F is also distributive.

These properties of field are inherited from the latter's progenitors, since the field is defined by the division ring which itself is defined by the ring which itself is defined by the group.

Table 1 shows the sources from which each of the properties of the field is defined.

operator	*property*	*defining definition*
addition	closed	group
	commutative	Abelian group
	associative	group
	identity	group
	inverse	group
multiplication	closed	ring
	commutative	commutative ring
	associative	ring
	identity	ring with identity
	inverse	division ring

Table 1 *The various sources at the places of which the various properties of the field are defined.*

Theorem 2. Consider any two elements a and b in a field F, we have $(-1)\cdot a = -a$.

Proof. Since,

$$(-1)\cdot a + a = (-1)\cdot a + a\cdot 1 = ((-1)+1)\cdot a = 0\cdot a = 0$$

and since $a + (-a) = 0$, therefore $(-1)\cdot a = -a$. ¶

Theorem 3. Let a and b be any two elements in a field F. Then $ab = 0$ implies $a = 0$ or $b = 0$.

Proof. If $a \neq 0$, then,

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b \cdot 1 = b$$

. And since a and b are arbitrary, and since $ab = ba$, our statement above is proved. ¶

Definition 5. Let a, b and m be integers, and let $m > 1$. Then a is said to be *congruent to b modulo m*, in other words,

$$a \equiv b (\mathrm{mod}\, m)$$

if $m|(a-b)$, that is to say, m divides $a-b$. The number m is called the *modulus*, and b is called the *residue* of $a(\mathrm{mod}\, m)$. Sometimes b is also called the *principal remainder* of a divided by m, and denoted by $(a(\mathrm{mod}\, m))$. A residue is said to be *common* if $0 \leq b < m$.

Theorem 4. Any integer a is congruent to exactly one of 0, 1, ..., $m-1$ modulo m.

Proof. Let a and m be integers, and let $m > 1$. Then there exists a unique k such that $a = mk + b$, where $0 \leq b \leq m-1$. Therefore b is uniquely determined by m and a.

To prove that b is unique, suppose there exist $a = mk_1 + b_1$ and $a = mk_2 + b_2$, where $0 \leq b_1 \leq m-1$ and $0 \leq b_2 \leq m-1$, such that $b_1 \neq b_2$. Then, $a - mk_1 \neq a - m_k 2$, and since $m > 1$, therefore $k_1 \neq k_2$. Since k_1 and k_2 are arbitrary, let $k_1 > k_2$ and let $k_1 = k_2 + n$. Then,

$$mk_2 + b_2 = a = m(k_2 + n) + b_1 = mk_2 + b_1 + mn$$

and since $b_1 \geq 0$, $m \geq 0$ and $n > 0$, we have $b_2 \geq m$, which contradicts what we have said earlier, that is $b_2 \leq m-1$. So, necessarily $b_1 = b_2$. ¶

Theorem 5. Let a, b and m are integers, and let $m > 1$. Then the following properties hold for congruence.

a. $a \equiv b (\mathrm{mod}\, 0)$ implies $a = b$

b. either $a \equiv b (\mathrm{mod}\, m)$ or $a \not\equiv b (\mathrm{mod}\, m)$

c. $m \equiv a (\mathrm{mod}\, m)$

d. $a \equiv b (\mathrm{mod}\, m)$ implies $b \equiv a (\mathrm{mod}\, m)$

e. if $a \equiv b (\mathrm{mod}\, m)$ and $b \equiv c (\mathrm{mod}\, m)$, then $a \equiv c (\mathrm{mod}\, m)$

Let $a \equiv b (\mathrm{mod}\, m)$ and $c \equiv d (\mathrm{mod}\, m)$. Then,

f. $a + c = b + d (\mathrm{mod}\, m)$

g. $a - c = b - d (\mathrm{mod}\, m)$

h. $ac = bd (\mathrm{mod}\, m)$

Further, let k and n be integers. Then,

i. if $a \equiv b (\mathrm{mod}\, m)$, then $ka \equiv kb (\mathrm{mod}\, m)$

j. if $a \equiv b (\mathrm{mod}\, m)$, then $a^n \equiv b^n (\mathrm{mod}\, m)$

k. if $a \equiv b (\mathrm{mod}\, m_1)$ and $a \equiv b (\mathrm{mod}\, m_2)$, then,

$$a \equiv b \,(\mathrm{mod}\, \mathrm{lcm}(m_1, m_2))$$

where $\mathrm{lcm}(x, y)$ is the least common multiple of x and y, that is the smallest z such that there exist positive integers p and q by which $px = qy = z$

l. if $a^k \equiv b^k (\mathrm{mod}\, m)$, then,

$$a \equiv b \left(\mathrm{mod}\, \frac{m}{\gcd(k, m)} \right)$$

From above properties, it follows that,

m. if $a \equiv b (\mathrm{mod}\, m)$, then $P(a) \equiv P(b) (\mathrm{mod}\, m)$, where $P(x)$ is a polynomial.

Properties (a) is called *equivalence*, (b) *determination*, (c) *reflexive*, (d) *symmetry*, and (e) *transition*.

Definition 6. We denote by $\mathbf{Z}_m$ or $\mathbf{Z}/(m)$ the set $\{0, \ldots, m-1\}$, where $m > 1$, and define the addition and multiplication on it as,

$$a \oplus b = (a + b (\mathrm{mod}\, m))$$

and

$$a \odot b = (ab (\mathrm{mod}\, m))$$

respectively, and these may be denoted as $a+b$ and respectively ab for simplicity.

Example 2. The set $\mathbf{Z}$ together with addition and multiplication introduced in Definition 6 form a ring.

Theorem 6. The ring $\mathbf{Z}_m$ is a field if and only if m is prime.

Proof. First we prove that m being prime implies that $\mathbf{Z}_m$ is a field. Let m be a prime. Then any $a \neq 0$ in $\mathbf{Z}_m$, in other words $0 < a < m$, is prime relative to m. Therefore, there exist two integers u and v, where $0 \leq u \leq m-1$, such that $ua + vm = 1$, which means that $ua \equiv 1 (\mathrm{mod}\, m)$. Hence $u = a^{-1}$, and since this applies for every a in $\mathbf{Z}_m$, it follows that $\mathbf{Z}_m$ is a field.

Next we will prove that if m is not a prime, then $\mathbf{Z}_m$ is no field. Suppose that m is not a prime. Then $m = ab$ for some a and b, where $1 < a < m$ and $1 < b < m$. But $ab = 0$ is in $\mathbf{Z}_m$, and therefore $a = 0$ and $b = 0$. This contradicts the values of a and b given above, thus $\mathbf{Z}_m$ is no field. ¶

Definition 7. We denote by na the element $\sum_{i=1}^{n}$ for any element a in a ring R and an integer $n \geq 1$.

§

Definition 8. Let F be a field. Then the *characteristic* of F is the least positive integer p such that $p \cdot 1 = 0$, where 1 is the multiplicative identity of F. Where no such p exists, this characteristic is defined to be zero.

By F^* we mean $F \backslash \{0\}$.

Theorem 7. The characteristics of a field is either zero or a prime number.

Proof. Consider a field F. Since $1 \cdot 1 = 1 \neq 0$, therefore 1 is not the characteristic of F. Let the characteristic be $p = mn$, where $1 < n < p$ and $1 < m < p$. If $a = m \cdot 1$ and $b = n \cdot 1$, then,

$$a \cdot b = (m \cdot 1)(n \cdot 1) = \left(\sum_{i=1}^{m} 1\right)\left(\sum_{j=1}^{n} 1\right) = mn \cdot 1 = p \cdot 1 = 0$$

This implies $a = 0$ and $b = 0$, which contradicts what we had assumed when we started. ¶

Definition 9. Let E and F be two fields, and let F be a subset of E. Then F is called a *subfield* of E if the addition and multiplication of E, when restricted to F, are the same as those of F.

Theorem 8. A finite field F of characteristic p contains p^n elements for some integer $n \geq 1$.

Proof. Choose an element α_1 from F^*. Then $0 \cdot \alpha_1, \ldots, (p-1) \cdot \alpha_1$ are pairwisely distinct from one another, for if $i \cdot \alpha_1 = j \cdot \alpha_1$ for some $0 \leq i \leq j \leq p-1$, then $(j-i) \cdot \alpha_1 = 0$. Since p is the characteristic of F, by Theorem 7 p can be either zero or prime. And since $0 \leq j - i \leq p - 1$, therefore $j - i = 0$, that is $i = j$. ¶

Next, if $F\backslash\{0\cdot\alpha_1,\ldots,(p-1)\cdot\alpha_1\}$ is not empty we choose from it α_2. Then $a_1\alpha_1+a_2\alpha_2$ are pairwise distinct for all $0\leq a_1,a_2\leq p-1$, for if $a_1\alpha_1+a_2\alpha_2$ for some $0\leq a_1,a_2,b_1,b_2\leq p-1$, then necessarily $a_2=b_2$ because otherwise,

$$\alpha_2=\frac{a_1-b_1}{b_2-a_2}\alpha_1$$

which contradicts the way we have chosen α_2. Then it follows that $(a_1,a_2)=(b_1,b_2)$.

Since F is finite, we may continue in this fashion to α_3, α_4, and so on until α_n for some integer n, and find α_j, for all $2 \leq j \leq n$, from $F \backslash \{\sum_{i=1}^{j-1} a_i \alpha_i\}$, where a_i, $i = 1, \ldots, j-1$, are in $\mathbf{Z}_p$.

In the end, $F = \{\sum_{i=1}^{n} a_i \alpha_i\}$, where $a_1, \ldots, a_n$ are in $\mathbf{Z}_p$. In the same manner as above, we may show that $a_1\alpha_1 + \ldots + a_n\alpha_n$ are pairwisely distinct from each other for all a_i in $\mathbf{Z}_p$, where $i = 1, \ldots, n$. Therefore $|F| = p^n$.

Definition 10. Let F be a field. Then the set,

$$F[x] = \left\{ \sum_{i=0}^{n} a_i x^i \right\}$$

where a_i is an element in F and $n \geq 0$, is called the *polynomial ring* over F. An element of $F[x]$ is called a *polynomial* over F. For a polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$, providing that $a_n \neq 0$, the integer n is called the *degree* of $f(x)$, denoted by $\deg(f(x))$. We define $\deg(0) = -\infty$. A nonzero polynomial $f(x)$ of degree n is said to be *monic* if $a_n = 1$. Furthermore, a polynomial $f(x)$ is said to be *reducible* over F if there exist two polynomials $g(x)$ and $h(x)$ over F such that $\deg(g(x)) < \deg(f(x))$ and $\deg(h(x))$, and $f(x) = g(x)h(x)$. A polynomial is said to be *irreducible* over F if it is not reducible.

Definition 11. Let $f(x)$ in $F[x]$ be a polynomial of degree $n \geq 1$. Then, for any polynomial $g(x)$ in $F[x]$ there exists a unique pair $(s(x), r(x))$ of polynomials, where $\deg(r(x)) < \deg(f(x))$ or $r(x) = 0$, such that $g(x) = s(x)f(x) + r(x)$. Here $r(x)$ is called the *principal remainder* of $g(x)$ divided by $f(x)$, or in our notation $(g(x)(\mathrm{mod}\, f(x)))$.

Definition 12. Let $f(x)$ and $g(x)$ in $F[x]$ be two nonzero polynomials. The *greatest common divisor* of $f(x)$ and $g(x)$, written $\gcd(f(x), g(x))$, is the monic polynomial of the highest degree which is a divisor of both $f(x)$ and $g(x)$. Two polynomials $f(x)$ and $g(x)$ are said to be *co-prime*, or *prime*, to each other if $\gcd(f(x), g(x)) = 1$. The *least common multiple* of $f(x)$ and $g(x)$, namely $\mathrm{lcm}(f(x), g(x))$, is the monic polynomial of the lowest degree which is a multiple of both $f(x)$ and $g(x)$.

Example 3. Let the factorisations of two polynomials $f(x)$ and $g(x)$ are,

$$f(x) = a \cdot (p_1(x))^{e_1} \cdots (p_n(x))^{e_n}$$

and

$$g(x) = b \cdot (p_1(x))^{d_1} \cdots (p_n(x))^{d_n}$$

where a and b are in F^*, and $e_i, d_i \geq 0$, and $p_i(x)$ are distinct monic irreducible polynomials, then,

$$\gcd(f(x), g(x)) = (p_1(x))^{\min(e_1,d_1)} \cdots (p_n(x))^{\min(e_n,d_n)}$$

and

$$\operatorname{lcm}(f(x), g(x)) = (p_1(x))^{\max(e_1,d_1)} \cdots (p_n(x))^{\max(e_n,d_n)}$$

Example 4. Let $f(x)$ and $g(x)$ in $F[x]$ be two nonzero polynomials. Then, there exist two polynomials $u(x)$ and $v(x)$ having $\deg(u(x)) < \deg(g(x))$ and $\deg(v(x)) < \deg(f(x))$ such that,

$$\gcd(f(x), g(x)) = u(x)f(x) + v(x)g(x)$$

Then,

$$\gcd(f(x)h(x), g(x)) = \gcd(f(x), g(x))$$

if $\gcd(h(x), g(x)) = 1$.

Theorem 9. Let $f(x)$ be a polynomial of degree n over a field F, where $n \geq 1$. Then $F[x]/(f(x))$, together with the addition,

$$g(x) \oplus h(x) = (g(x) + h(x) (\mathrm{mod}\, f(x)))$$

also written $g(x) + h(x)$, and multiplication,

$$g(x) \odot h(x) = (g(x)h(x) (\mathrm{mod}\, f(x)))$$

also written $g(x) \cdot h(x)$, form a ring. Furthermore, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Example 5. Consider the ring $\mathbf{Z}_2[x]/(1+x^2) = \{0, 1, x, 1+x\}$ Its addition and multiplication tables are shown in Table 2.

$+$	0	1	x	$(1+x)$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\times$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	1	$1+x$
$1+x$	0		$1+x$	0

Table 2 *Addition and multiplication tables for* $\mathbf{Z}_2[x]/(1+x^2)$.

Example 6. Consider the ring $\mathbf{Z}_2[x]/(1+x+x^2)$. Its addition and multiplication tables are given in Table 3.

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\times$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Table 3 *Addition and multiplication tables for* $\mathbf{Z}_2[x]/(1+x+x^2)$.

Example 7. Table 4 shows the analogies between $\mathbf{Z}$ and $F[x]$.

the integral ring $\mathbf{Z}$	the polynomial ring $F[x]$
an integer m	a polynomial $f(x)$
a prime number p	an irreducible polynomial $p(x)$
$\mathbf{Z}_m = \{0, \ldots, m-1\}$	$F[x]/(f(x)) = \{\sum_{i=0}^{n-1} a_i x^i; a_i \in F, n \geq 1\}$
$a \oplus b = (a + b (\mathrm{mod}\, m))$	$g(x) \oplus h(x) = (g(x) \oplus h(x) (\mathrm{mod}\, f(x)))$
$a \odot b = (ab (\mathrm{mod}\, m))$	$g(x) \odot h(x) = (g(x)h(x) (\mathrm{mod}\, f(x)))$
$\mathbf{Z}_m$ is a ring	$F[x]/(f(x))$ is a ring
$\mathbf{Z}_m$ is a field if and only if m is a prime	$F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible

Table 4 *Analogies between* $\mathbf{Z}$ *and* $F[x]$.

Theorem 10. For every element ϕ of a finite field F with n elements, $\phi^n = \phi$.

Proof. The case when $\phi = 0$ is trivial. Next, if $\phi \neq 0$, then we could list all the nonzero elements of F as $F^* = \{\phi_1, \ldots, \phi_{n-1}\}$. And since F is closed, we could multiply each element in F^* to obtain $F^* = \{\phi\phi_1, \ldots, \phi\phi_{n-1}\}$. Therefore $\phi_1 \cdots \phi_{n-1} = (\phi\phi_1) \cdots (\phi\phi_{n-1})$, which leads to $\phi^{n-1} = 1$. ¶

Corollary 10[1]. Let F be a subfield of E, and let $|F| = n$. Then an element ϕ of E is also in F if and only if $\phi_n = \phi$.

Proof. The *if* part was already proved in Theorem 10. For the *only if* part, if ϕ satisfy $\phi^n = \phi$, then it is a root of $x^n - x$. And since $|F| = n$ means that all the elements of F are roots of $x^n - x$, it follows that ϕ lies in F. ¶

Definition 13. We denote a finite field with q elements by $\mathbf{F}_q$ or $GF(q)$. Let α be a root of an irreducible polynomial $f(x)$ of degree n over a field F. Then, if we replace x in $F[x]/(f(x))$ by α, the field $F[x]/(f(x))$ can be represented as,

$$F[\alpha] = \{\sum_{i=0}^{n-1} a_i \alpha^i\}$$

for a_i in F.

Definition 14. An element α in a finite field $\mathbf{F}_q$ is called a *primitive element*, or *generator*, of $\mathbf{F}_q$ if $\mathbf{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.

§

Definition 15. The *order*, $\mathrm{ord}(\alpha)$, of a nonzero element α in $\mathbf{F}_q$ is the smallest positive integer k such that $\alpha^k = 1$.

§